CSC-EPL-91/004

(2)

NATIONAL COMPUTER SECURITY CENTER

FINAL EVALUATION REPORT

OF

AMERICAN COMPUTER SECURITY INDUSTRIES, !NC.

COMPSEC - II

10 June 1991

Approved for Public Release:
Distribution Unlimited

FINAL EVALUATION REPORT

American Computer Security Industries, Inc.

COMPSEC-II

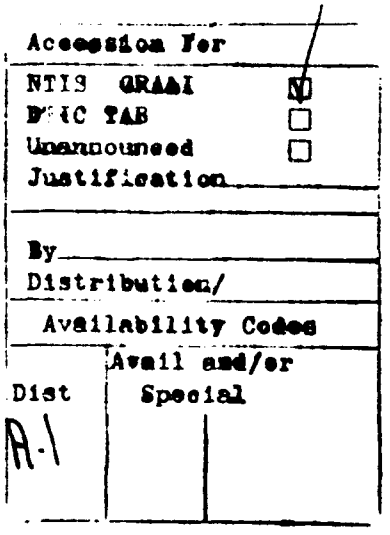
NATIONAL

COMPUTER SECURITY CENTER

9800 Savage Road
Fort George G. Meade
Maryland 20755-6000

10 June 1991

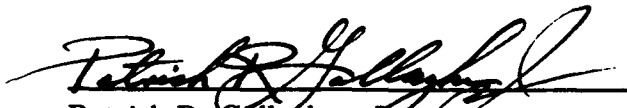
CSC-EPL-91/004
Library No. S236,004



FOREWORD

This publication, the Final Evaluation Report of A.C.S.I. Inc.COMPSEC-II is being issued by the National Computer Security Center under the authority of and in accordance with DoD Directive 5215.1,"Computer Security Evaluation Center." The purpose of this report is to document the results of the A.C.S.I. Inc. evaluation. The requirements stated in this report are taken from the *Computer Security Subsystem Interpretation* of the *Department of Defense Trusted Computer System Evaluation Criteria* dated 16 September 1988.

Approved:



Patrick R. Gallagher, Jr.
Director
National Computer Security Center

10 June 1991

ACKNOWLEDGEMENTS

Team Members

Team members included the following individuals, who were provided by the following organization:

Barbara A. Maguschak
Cynthia Reese
Robert L. Williamson

The MITRE Corporation
7525 Colshire Drive
McLean, Virginia 22102

Trusted Product and Network Security Evaluation Division
National Security Agency
Fort George G. Meade, Maryland 20755

Contents

EXECUTIVE SUMMARY

The National Security Agency (NSA) / National Computer Security Center (NCSC) examined the security protection mechanisms provided by American Computer Security Industries, Inc.'s COMPSEC-II. COMPSEC-II is a subsystem, not a complete trusted computer system. It was therefore evaluated against the *Computer Security Subsystem Interpretation* (CSSI) of the *Trusted Computer System Evaluation Criteria* (TCSEC). The computer security features evaluated were discretionary access control (DAC), object reuse (OR), identification and authentication (I&A), and audit (AUD).

The evaluation team determined that the highest rating at which COMPSEC-II satisfies the DAC, OR, I&A, and audit requirements of the CSSI is class D. The D rating in each of the rated components resulted from COMPSEC-II's inability to meet all feature, assurance, and documentation requirements specified by the CSSI. See page 38, "Rating Assignment", for a description of the elements in each rating category.

COMPSEC-II should be protected from the system it is helping to augment by controlling those programs and utilities that are capable of compromising COMPSEC-II. That includes programming languages, compilers, debuggers, COMPSEC-II's utilities, and other unspecified applications programs. The system operator should restrict access to these programs and utilities by using COMPSEC-II's DAC protection mechanism. However, this alone will not necessarily prohibit users from installing their own programs and utilities.

Subsystems are intended to add a level of assurance to an automatic data processing (ADP) system that has limited or ineffective security mechanisms. Subsystems are not intended to protect any information on an ADP system which processes classified information because subsystems may not be capable of maintaining the integrity of classified information. Subsystems should not be added to an ADP system for the sole purpose of processing classified or sensitive information.

Introduction

This evaluation applies to COMPSEC-II available from American Computer Security Industries, Inc.

In December 1989, the evaluation team began a product evaluation of the COMPSEC-II product as configured for the IBM-PC and compatibles. The objective of this evaluation was to rate COMPSEC-II against the *Computer Security Subsystem Interpretation* (CSSI) of the *Trusted Computer System Evaluation Criteria* (TCSEC) and to place it on the Evaluated Products List (EPL) with a final rating for each of COMPSEC-II's evaluated features. This report documents the results of the evaluation.

Material for this report was gathered by the COMPSEC-II evaluation team through documentation review, interaction with company representatives, and through the actual use and testing of COMPSEC-II.

Evaluation Process Background

The National Computer Security Center (NCSC), located within the National Security Agency (NSA), was created to improve the state of computer security in computer systems processing information that is vital to the owners of that information. The Center fulfills its mission by promoting the development and implementation of trust technology and encouraging the widespread availability and use of trusted computer security products. Through the Trusted Product Evaluation Program (TPEP), the Center works with the manufacturers of hardware and software products to implement and make available to the public technically sound computer security solutions. Under this program, the Trusted Product and Network Security Evaluation Division evaluates the technical protection capabilities of computer security products against well-defined published evaluation criteria.

The product evaluation process culminates in the publication of a Final Evaluation Report, of which this document is an example. The Final Evaluation Report describes the product and assigns it a rating that denotes a specific level of trust. The assigned rating is independent of any consideration of overall system performance, potential applications, or particular processing environment. Rated products are listed on the Evaluated Products List (EPL), the aim of which is to provide ADP system developers, managers, and users an authoritative evaluation of a product's suitability for use in processing important information.

Subsystem Evaluation Program

The NCSC has recognized a need for guidance on, and evaluation of, computer security products that do not meet all of the feature, architecture, or assurance requirements of any one security class of the TCSEC. The NCSC has, therefore, established a Computer Security Subsystem Evaluation Program.

The goal of the Computer Security Subsystem Evaluation Program is to provide computer installation managers with information on subsystems that would be helpful in providing immediate computer security improvements to existing installations.

Security Managers should note that subsystems are not capable of protecting information with sufficient assurance to maintain classified information on a system protected solely by security subsystems. Furthermore, subsystems may not be used to upgrade the protection offered by complete trusted systems for the sole purpose of adding the ability to store or process classified material. Subsystems may be added to other protection devices to provide another layer of security, but in no way may be used as justification for processing classified material.

Subsystems considered in the subsystem evaluation program are special purpose products that can be added to existing computer systems to increase some aspect of security and have the potential of meeting the needs of both civilian and government departments and agencies. For the most part, the scope of a computer security subsystem evaluation is limited to consideration of the subsystem itself, and does not address or attempt to rate the overall security of the processing environment.

To promote consistency in evaluations, subsystems' security mechanisms are assessed against the *Computer Security Subsystem Interpretation* (CSSI) of the *Trusted Computer System Evaluation Criteria.* Additionally, the evaluation team reviews the vendor's claims and documentation for obvious flaws which would violate the product's security features, and verifies, through functional testing, that the product performs as advertised. Upon completion, an evaluation report will assign a specific rating for each of the components of the subsystem and a summary of the evaluation report will be placed on the Evaluated Products List (EPL) which is maintained in the *Information Systems Security Products and Services Catalog.*

Document Organization

This report consists of four chapters and three appendices. Chapter 1 is this introduction. Chapter 2 provides an overview of the system's hardware and software architecture and a

description of the security features provided by COMPSEC-II. Chapter 3 provides a mapping between the requirements specified in the CSSI and the features and assurances that fulfill those requirements. Chapter 4 presents the evaluation team's comments on the subsystem. The first two appendices identify the hardware and software components that specify the configuration to which this evaluation applies. The final appendix is a list of acronyms.

System Overview

Product History

American Computer Security Industries, Inc. (A.C.S.I. Inc.) is a manufacturer of security products for desktop, laptop and telecommunications environments.

This evaluation is of the "COMPSEC-II USA American Version" of COMPSEC-II, release B3.1, installed as recommended by the Operations Manual to provide the maximum security offered by the product. This version is intended for American use. The versions intended for international and export use, "COMPSEC-II EEC International Version"and "COMPSEC-II AZ International Version with AZERTY" were not evaluated.

Product Overview

COMPSEC-II is a hardware based product for use in microcomputers. COMPSEC-II release B3.1 was evaluated with multiple defined users in the configuration supplied for the IBM-PC. It allows up to nine users plus a system operator to share a single terminal on an IBM-PC, XT, AT, or compatible machine running DOS versions 2.0 through 3.3. Throughout this report the term "user" will be used to refer to a regular unprivileged user. The term "system operator" will be used to refer to the one user that is permitted to access all system resources.

COMPSEC-II is a combined hardware and software product on a hardware card providing real-time access control to system resources and processing of audit data. A menu-driven utility program for configuring and monitoring the system is also provided.

Initial installation involves inserting the hardware card in an available slot on the computer's motherboard and then running an installation program which creates a directory on the hard disk drive and copies the COMPSEC-II files to this directory. The target system must have a hard disk drive and must be capable of using double-sided diskettes with 360K of storage.

This product can also be used in a network environment but was not evaluated in that configuration.

Security Relevant Portion (SRP)

The protection critical mechanisms or the Security Relevant Portion (SRP) of COMPSEC-II is implemented in both hardware and software. A description of these mechanisms and their security relevant roles is in the following sections.

Hardware Architecture

The hardware base of COMPSEC-II consists of a hardware card that is inserted in an available circuit board slot on an IBM-PC, IBM-XT, IBM-AT, 386-based machine, or a 100% compatible computer. The card is designed to be mapped to a fixed location in memory. Dip switches on the board designate the location of the card and assure that it will not be in contention for space with other cards.

The card is mapped to 8K bytes of memory and provides write-protected RAM for COMPSEC-II program storage, additional RAM for temporary data and stack storage, a write-protected real-time clock, a Data Encryption Standard (DES) chip, two groups of write-protected storage registers for DES key storage and a control register that forms the index to the two groups of storage registers. The control register is also used to set and clear the write-protect flag to the protected devices (clock, storage registers, and program RAM) on the COMPSEC-II card. All accesses to the COMPSEC-II card are through memory read and write operations.

The COMPSEC-II card also includes a battery which supplies power to the real-time clock and to the RAM on the card. The date and time from this clock are used in the audit log time stamps.

When MS-DOS is loaded during a normal boot procedure, the MS-DOS file **config.sys** is opened as part of this load sequence. This file allows the user to customize the MS-DOS environment. The COMPSEC-II installation program modifies **config.sys** by adding a line to define the file **acd.sys** as a device driver. This file is COMPSEC-II's access control driver. Each time the system is booted, **config.sys** loads the driver into memory. Once the COMPSEC-II installation program has modified **config.sys**, it then hides **config.sys** so that users have no access to this file through DOS or BIOS commands. Users cannot unhide this file or obtain any information about it through the use of the DOS attribute command. This prohibits a user from editing **config.sys** and removing the initialization of COMPSEC-II's device driver.

Software Architecture

The software architecture of COMPSEC-II combines software with a menu-driven utility program, **compsec.exe**. All administration and configuration of security relevant options are done by the system operator through this utility program.

Once the hardware card has been installed in the PC, the system operator then installs the software portion of the system. This is done by running the installation program that is on the supplied diskette. At this time the system operator establishes the account information for the system operator including logon name, password, group and user number, and valid days and times for logon. The setting of the clock on the COMPSEC-II card is also initialized at this time. Any future changes to be made to the clock must be done through a menu option in the **compsec.exe** utility program.

The system operator then configures the system by changing to the `c:\compsec` directory and running **compsec.exe**. This will put the system operator into the menu-driven utility program. By default, the initial DAC configuration that is supplied with the system is that the system operator is the only user that has access to this directory. Additionally, to enter the utility program, the system operator must be re-authenticated to the system by entering the system operator's logon name and password.

Security Relevant Options

The security relevant options that must be set on COMPSEC-II include both switches and menu options. The switches that must be set by the system operator include:

time-out Set an automatic time-out value to force logout after specified amount of time that keyboard is idle. Valid values are 0-30 minutes where 0 disables the automatic logout feature.

key off Allow a user to lock the system without logging off. This feature is keyboard specific and could not be tested during this evaluation.

exit off The vendor also refers to this as the Application Logoff switch. The user is automatically logged out upon completion of the first user application run after the initial logon. The user must logon again prior to the execution of any additional applications.

auto on Allow a user to automatically log on as "group 9" where this group does not require authentication. This feature must be disabled for the evaluated system as it does not provide unique identification of users nor does it provide for authentication of the users, and it provides no way of identifying the user during the auditing of the user's actions.

mod exe's This switch is meant to prevent modifications to executable files. It prevents the deletion and restricts the creation of files where the file name ends in **.exe**. However, the system does allow creation of a file with the **.exe** suffix through the use of the DOS *rename* command if the original filename did not end in **.exe**. Although the Operations Manual does not make any mention of it, COMPSEC-II enforces these same restrictions on **.com** files as well.

direct Allow or deny direct disk access. If direct disk access is blocked then direct BIOS calls to any of the disk sectors is blocked for users. This will prevent the use of utilities such as Norton that read and write directly to the disk.

reboot This is the switch for object reuse to determine if the system will clear the memory and reboot the system on each user change. Files are always overwritten upon deletion, regardless of the setting of this switch. (See page 11, Object Reuse.)

vectors Cause COMPSEC-II to scan the interrupt vectors for any changes. The evaluation team was not able to determine what COMPSEC-II does in the event of a change to the interrupt vectors.

initial Allow the system operator to specify an initial logon command sequence for each of the nine users so that when the user logs on, this command sequence is executed before the user gains control of the system. This feature may be used to change a user's working directory to a specified area or to invoke a specific application such as a spread sheet or database.

boot protection - Allow the system operator to specify that the system can only be booted from drive C thereby disallowing a user from booting the system from a standard DOS bootable diskette which would bypass the COMPSEC-II security features.

SYS.ID Specify the system id that must be used by the system operator to regain access to the system if the COMPSEC-II hardware is removed from the system.

It is possible for the system operator to select options that will allow protection of the C drive if the COMPSEC-II hardware is removed. If the system operator both selects C as the boot drive and sets the boot protection option, then if the COMPSEC-II hardware is removed, the system will not be able to access the C drive. To recover the C drive, the system operator must boot the system from a floppy disk drive and run a program from the floppy that was used to install COMPSEC-II. This procedure requires that the system operator be identified and authenticated by entering the system operator's logon name, password, and the SYS.ID.

The following are the menu options that the system operator can select.

Adding Users Allows the system operator to add users. The Operations Manual states that there is a limit of nine users plus the system operator. However, the system that we received and tested allowed up to 50 users. The system must be limited to nine users plus the system operator to meet the D2 DAC requirement. (See page 10, Discretionary Access Control, for further restrictions.) The system operator sets each user's logon name and password. The system operator may allow a user to set their own initial password; however, once set, users may not change their own passwords - only the system operator may change a password for any user. The logon name and password are used by the I&A mechanism to validate the user for logging in to the system.

Valid days and times can be set individually for each user thereby limiting the time that they may gain access to the system. If a user is logged in when they reach an invalid time, they will be logged off the system. The system operator may specify a date on which a user's account will expire. The user will be warned as this date approaches.

The system operator may give each user access to the manual encryption/decryption and message authentication facilities. (See page 33, Security Features User's Guide.)

File Access COMPSEC-II has a menu option to set the access on files, directories, and disk drives. Only the system operator has access to this utility; that is, users cannot set the access on their own files. (See page 10, Discretionary Access Control.)

Audit The final evaluated menu option is for handling the audit information. The system operator uses this menu option to enable/disable auditing, view the audit logs, and clear the audit logs. (See page 14, Audit.)

SRP Protected Resources

This section describes the subjects and objects that COMPSEC-II mediates access between.

Subjects

The subjects are those processes that act on behalf of the users. A process is the abstraction of tasks which comprise a program. It consists of the current value of the program counter, registers, and associated variables. On a PC running MS-DOS in real mode, all user processes execute in a single state. There is no state separation for processes. It is the responsibility of subjects (e.g. programs) not to interfere with one another.

Access to the COMPSEC-II utilities is controlled by password in the same manner as the system itself, however, once access is granted, they are subjects acting on behalf of a user (the system operator), as is any other program.

Objects

COMPSEC-II's protected objects include the following named objects and storage objects.

The named objects are:

- Files
- Directories
- Serial Ports
- Parallel Ports
- Floppy Disk Drives

The storage objects are:

- Files
- Directories
- Addressable RAM
- Memory - including extended/expanded memory

SRP Protection Mechanisms

This section describes COMPSEC-II's privileges, DAC, object reuse, I&A, and audit mechanisms.

Privileges

COMPSEC-II is installed with only one privileged user, the system operator, who has the ability to implement administrative capabilities. To do so, the system operator executes **compsec.exe**. The system operator must enter the logon name and password each time the *compsec* command is issued. This program allows the system operator to control the DAC, OR, I&A and audit mechanisms.

Discretionary Access Control

COMPSEC-II provides maintenance of the discretionary access controls (DAC) through an Access Control Editor that is accessed by executing the *compsec* command.

COMPSEC-II controls access to some objects (the serial and parallel ports) by permitting only the system operator to print files. The remaining objects that are controlled by COMPSEC-II are directories, disk drives and files. The access that a user is permitted to an object is determined by the user's group id. This group id is different from the user's logon name that is used for identification and authentication during the logon process. Discretionary access is controlled for up to ten groups. Groups are given discretionary access to named objects by the system operator, who is assigned to group 0 when COMPSEC-II is installed. The system can support up to ten users and up to ten groups. To have DAC at the granularity of a single user, only one user can be assigned to a group.

When the **compsec.exe** program is first executed, the only initially secured object is the `c:\compsec` directory in which this product resides. Access to this directory is limited to the system operator, who is the first user to access the system. The initial user interface allows only an access mechanism which forces the first user to establish user identities and roles.

Access to every object afforded any one of the up to ten groups is controlled through an access control matrix that is established by the system operator. Each named object has an entry in this matrix. Named objects are identified using the Access Control Editor. Every identified named object has an access entry for every one of the up to ten groups on the system.

Six types of access are allowed to an object. They are shown in Table 2.1.

Access to any object can be granted to a user by the system operator when the system operator logs on. The system operator initially is presented with a "System Access Control Menu" with four choices: "Help", "Users", "Files", and "Quit". If "Files" is chosen, the Access Control Editor is invoked and the file that contains the access control matrix for all

Access Types	Permissions		
	Read	Write	Execute
Unlimited "U"	X	X	X
No Access "N"			
Read Only "R"	X		
Execute Only "E"			X
No Execute "X"	X	X	
Write Only "W"		X	

Table 2.1: Access Types

named objects may be accessed. Access may be specified for an entire directory of files, individual files, or a disk drive. Each group is given one of the types of access (as defined in Table 2.1) to each object that is in the matrix.

The DAC mechanism also supports access exclusion whereby subjects may be denied access to all objects except those to which the user is given specific access.

Various options are provided by the Access Control Editor. For each object, the system operator can specifiy that each time the specified object is opened, the user must again revalidate his identity (see page 12, Identification and Authentication). A similar option is available for executable files so that every time a user with execute privilege attempts to execute the file, that user's logon name and password must be revalidated to the system. Encryption options also are available, but these were not reviewed.

Object Reuse

COMPSEC-II provides two different mechanisms to implement object reuse for the different types of storage objects. Object reuse for the deletion of files is always in force but the system operator must select object reuse for internal storage objects.

Files

COMPSEC-II provides a file erasure feature which is always in force. Upon file deletion, there is a complete overwrite with blocks of random characters so that the original contents of the file are destroyed. It is undocumented what happens to a directory structure when it is deleted.

Internal storage objects

For object reuse to be effective for internal storage objects, the system operator must select the **System Reboot Enabled** option from within the Operations Update menu of **compsec.exe**. If this option has been selected, then when a user executes the *logoff* command, the system performs a full reboot which clears RAM, TSRs, buffers (not identified) and registers (not identified). If a user does not execute *logoff* because the timed keyboard logoff was executed or trouble with the system forced the system operator to logon, then the system will not reboot until a different user attempts a logon sequence.

Removable media

The only removable media on the configurable hardware are floppy disks mounted on a floppy disk drive.

The system operator can deny access to the floppy disk drives for any selected users. The system operator may allow access to the floppy disk drive only for specific executable files, also on a per user basis. Additionally, the operator can set the file access control parameters so that all files on the floppy disk drives must be encrypted and belong to the user attempting access. This feature is designed to preclude the use of data from floppies imported from other systems by anyone other than the operator. This is important because COMPSEC-II does not erase the contents of a floppy disk before writing to it.

Identification and Authentication

COMPSEC-II enforces Identification and Authentication (I&A) of users before users are allowed to access the system upon which it is installed. After the system is booted, the user is always greeted with a Logon Screen, which is a welcome message, the day of the week and the time, and a logon prompt.

The system operator configures the system and sets the security parameters through a menu-driven program in the `c:\compsec` directory named **compsec.exe**. I&A is implemented through the configuration of the Access Control Area, specifically the Logon Control Menu which is accessed by executing the *compsec* command. Only the system operator is allowed to access the Logon Control Menu.

The `c:\compsec` directory is hidden from users unless the system operator wishes to give access to users. The only time a user would need access to the `c:\compsec` directory is if the system operator gives that user the ability to encrypt files. With the encryption capability,

a user can run *compsec* with the ability to use only the encryption utilities. The operations manual recommends that access to the `c:\compsec` directory and the ability to encrypt files be restricted to the system operator.

Various menus can be accessed within **compsec.exe**. Before access is given to each menu, with the exception of the encryption menu, I&A of the user is enforced to reverify that the user is the system operator. Besides the encryption capability, which is given to only specified users, all other features within **compsec.exe** can be accessed only by the system operator.

In the Logon Control Menu, the system operator must enter the following required information for each user: logon name, password, restriction of access to specific days of the week and times of the day (default is unlimited access), group number, ability to encrypt own files (default is no), and expiration date of password (default is none). COMPSEC-II assigns each user a unique user number. Auditable events are associated with this user number. The maximum number of users allowed is ten, including the system operator, and the maximum number of groups is ten. The system operator must always be assigned to Group 0.

To access the system, at the Logon Screen, a user must first give a logon name followed by a password to authenticate the logon name. The Operations Manual claims that the system operator can create a password for a user or can allow a user to create a password. However, the system we tested did not allow the system operator to add a user without a password. There is a random key generator available for password generation based on the current system time. A logon name may consist of up to 16 characters with no minimum. However, the Operations Manual recommends that the logon name be a minimum of six characters. A password may consist of up to 16 characters with a minimum of six. However, the system operator can create passwords shorter than six characters.

There are several options that COMPSEC-II provides that involve I&A. All of these options can be set only by the system operator. In configuring the discretionary access control mechanism, COMPSEC-II provides a Validate User option by which the system operator can grant access to a user which requires that user to re-validate that user's logon name and password for opening or executing a file.

COMPSEC-II enforces I&A after the Dual Key Logoff feature is utilized. The Dual Key Logoff feature is an optional feature which allows a user to quickly lock the system allowing only authorized access thereafter. The system can be locked by either depressing "ctrl +" or "ctrl -". "ctrl +" will allow only the same user to log on having access to the file that was previously in use. "ctrl -" will allow any user to log on with System Reboot enforced.

Automatic Keyboard Time-out is another optional feature provided by COMPSEC-II. By selecting Time-out, the system operator sets the amount of time that the keyboard may

remain inactive before the user will be automatically logged off. The system operator may select a time from 0 to 30 minutes. After the designated time period has elapsed without keyboard activity, the user is logged off. Only the system operator or the original user may log back onto the system. Object Reuse is then not neccessary, thus not enforced.

COMPSEC-II provides an option that allows Automatic Logon to Group 9. When the system operator sets the auto logon option, after the system power has been turned off and then back on, if the user pauses ten seconds at the Logon Screen without any keyboard activity, that user will automatically be logged on as user group 9 with all rights that are assigned to that user group. However, to meet the D2 security requirements for I&A this option can not be allowed because it does not provide for individual accountability and authentication of group 9 users.

The SYS.ID option allows customization of an individual computer. A unique identifier (SYS.ID) may be entered by the system operator into the Hard Drive Protection Menu within **compsec.exe**. This SYS.ID must be entered, along with the system operator's logon name and password before any system authorization is permitted.

Application Logoff is an option which if chosen by the system operator will force a user to be logged off upon exit of the first user application run after logon. This ensures that the user has access to only the first application file that is run after logon. The system operator could additionally set an initial logon sequence for each group which would automatically execute a specified application file when that group logs on.

Audit

COMPSEC-II has the capability to record events in an audit trail and generate a report. Two audit records are maintained, one for a history of logons and logon attempts and the other is an audit trail of all commands executed at the DOS command level.

Each entry in the audit record of logon attempts includes:

- logon name used
- date
- time
- success or failure of logon attempt

The audit trail file of DOS-level commands is chronological. The entry for a login or logoff event shows the user number and date and time of the event. Following a login, all subsequent

commands are assumed as being entered by that user until reaching an audit trail entry for a logoff command. Each of the remaining entries in the audit trail file contains the following information:

- DOS command name
- any associated system calls
- pathname including directory and filename
- number of reads and writes performed on opened files
- date
- time

None of the actions that are taken while running the **compsec.exe** utility program are shown in the audit trail, only the entrance and exit of this program. Therefore, no system and security relevant actions taken by the system operator from within **compsec.exe** are audited. This includes such things as adding and deleting users, setting user access on files and directories, setting security relevant switches such as boot protection and modifications to the system clock, as well as any actions taken on the audit trail itself.

The file of audit records, `c:\compsec.adt`, is encrypted and hidden using the DOS attribute facility.

There are no pre-selection criteria for generating the audit records. The system operator views the audit records using the **compsec.exe** utility program. The audit records can be either viewed on the screen or a report can be generated for viewing. While viewing the audit records on the screen, the system operator has the ability to search for strings to selectively view the audit information. If a report is generated, it can be either directed to a specified file or it can be sent to a printer. If the report is saved in a file, the system operator could use an editor to view the records.

The system clock resides in the hardware of the card provided by COMPSEC-II and can only be accessed through the execution of the **compsec.exe** utility program. Therefore, users are prevented from modifying the system clock ensuring that an unprivileged user cannot tamper with the date and time stamps in the audit trail.

The system operator determines the amount of memory in bytes that is reserved for the audit trail. If an unprivileged user is logged on when this threshold is reached, the system disallows any further processing of commands and instructs the user to logoff and advise the system operator of the situation. The only action that is permitted at this time is for the

user to logoff. If any user other than the system operator attempts to logon at this time, the system will advise that user that the audit trail is full and that only the system operator can log on. When the system operator logs on, the system automatically allocates an additional 5000 bytes of memory for the audit trail. If the system operator does not clear the audit trail or allot more space before again filling the audit area, the system operator is told to logoff and log back on as system operator. The process of allocating 5000 more bytes repeats itself.

The system operator can disable auditing by entering a size of 0 for the audit trail. This is something the system operator should never do.

Evaluation as a Subsystem

This chapter presents the CSSI requirements (and interpretations) for the features that were evaluated. The computer security features that were evaluated for the COMPSEC-II product are Discretionary Access Control (DAC), Object Reuse (OR), Identification and Authentication (I&A) and Audit. For each feature, this chapter states the requirements, describes COMPSEC-II's efforts to meet those requirements, and concludes with a statement as to the level of requirements that have been satisfied. This pattern is continued for each of the CSSI requirements for assurance and documentation. Finally, a rating assignment section (see page 38 "Rating Assignment") describes how the various individual ratings for features, assurances, and documentation combine to form a composite rating for each evaluated feature.

Features

Discretionary Access Control

Requirement

The TCB shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined groups of individuals, or by both, and shall provide controls to limit propagation of access rights. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

Interpretation

- D1:

In the TCSEC quote, "TCB" is interpreted to mean "DAC subsystem".

2.1.3.1.1 Identified users and objects

DAC subsystems must use some mechanism to determine whether users are authorized for each access attempted. At DAC/D1, this mechanism must control access by groups of users. The mechanisms that can meet this requirement include, but are not limited to: access control lists, capabilities, descriptors, user profiles, and protection bits. The DAC mechanism uses the identification of subjects and objects to perform access control decisions. This implies that the DAC subsystem must interface with or provide some I&A mechanism. The evaluation shall show that user identities are available to DAC.

2.1.3.1.2 User-specified object sharing

The DAC subsystem must provide the capability for users to specify how other users or groups may access the objects they control. This requires that the user have a means to specify the set of authorizations (e.g., access control list) of all users or groups permitted to access an object and/or the set of all objects accessible to a user or group (e.g., capabilities).

2.1.3.1.3 Mediation

The checking of the specified authorizations of a user prior to granting access to an object is the essential function of DAC which must be provided. Mediation either allows or disallows access.

- D2:

The following interpretations, in addition to the interpretations for the DAC/D1 Class, shall be satisfied at the DAC/D2 Class.

2.1.3.2.1 Single-user access granularity

The DAC/D2 class requires individual access control; therefore, the granularity of user identification must enable the capability to discern an individual user. That is, access control based upon group identity alone is insufficient. To comply with the requirement, the DAC subsystem must either provide unique user identities through its own I&A mechanism or interface with an I&A mechanism that provides unique user identities. The DAC subsystem must be able to interface to an auditing mechanism that records data about access mediation events. The evaluation shall show that audit data is created and is available to the auditing mechanism.

2.1.3.2.2 Authorized user-specified object sharing

The ability to propagate access rights to objects must be limited to authorized users. This additional feature is incorporated to limit access rights propagation. This distribution of privileges encompasses granting, reviewing, and revoking of access. The ability to grant the right to grant propagation of access will itself be limited to authorized users.

2.1.3.2.3 Default protection

The DAC mechanism must deny all users access to objects when no explicit action has been taken by the authorized user to allow access.

Applicable Features

COMPSEC-II identifies and authenticates individual users. However, in the vendor's documentation, discretionary access controls are described at the granularity of a group. Even though the documentation does not specify that only one user can be assigned to a group, if the system is administered this way, COMPSEC-II meets the D2 requirement for single-user access granularity for DAC. Otherwise, COMPSEC-II meets the D1 requirement for controlling a user's access to objects.

The system operator is the owner of all named objects on the system. Only the system operator has access to the **compsec.exe** utility and all discretionary access to named objects is controlled through the use of this utility. Therefore, COMPSEC-II meets the D1 requirement that user(s) can specify how other users or groups access objects under owner control.

Only the system operator can grant discretionary access to any system object. Therefore, COMPSEC-II meets the D2 requirement that only authorized users can propagate access rights to objects.

To provide default protection such that all users are denied access to objects when no explicit action has been taken to allow access, the system must be configured as described in the vendor's operations manual for Master Exclusion Access Control. Under this configuration, all users other than the system operator are denied access to all objects except those objects to which specific access is given.

Conclusion

COMPSEC-II satisfies the D2 requirement for DAC.

Object Reuse

Requirement

All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system.

Interpretation

- D2:

In the TCSEC quote, "TCB" is interpreted to mean "protected system". Otherwise, this requirement applies as stated. The object reuse subsystem shall perform its function for all storage objects on the protected system that are accessible to users.

Applicable Features

Deleted files are overwritten by COMPSEC-II with what appears to be encrypted data or random characters. This feature is always enforced. COMPSEC-II can be configured so

that when a user executes the *logoff* command or if a different user logs in, COMPSEC-II performs a full reboot which clears RAM, TSR's, registers, and buffers.

COMPSEC-II does not provide any object reuse protection on removable media (floppy disks). Therefore, access to floppy disk drives must be restricted to the system operator. Alternatively, there can be a procedure enforced that requires that all floppy disks be degaussed or otherwise erased before they are issued to users.

Conclusion

COMPSEC-II satisfies the D2 requirement for object reuse.

Identification and Authentication

Requirement

The TCB shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

Interpretation

- D1:

The I&A subsystem shall require users to identify themselves to it before beginning to perform any other actions that the system is expected to mediate. Furthermore, the I&A subsystem shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The I&A subsystem shall protect authentication data so that it cannot be accessed by any unauthorized user.

The I&A subsystem shall, at a minimum, identify and authenticate system users. At I&A/D1, users need not be individually identified.

- D2:

The following interpretations, in addition to those interpretations for I&A/D1, shall be satisfied at the I&A/D2 Class.

In the TCSEC quote, "TCB" is interpreted to mean "I&A subsystem." The I&A subsystem shall pass the protected system a unique identifier for each individual.

The I&A subsystem shall be able to identify each individual user. This includes the ability to identify individual members within an authorized user group and the ability to identify specific system users such as operators, system administrators, etc.

The I&A subsystem shall provide for the audit logging of security relevant I&A events. For I&A, the origin of the request (e.g. terminal ID, etc.), the date and time of the event, user ID (to the extent recorded), type of event, and the success or failure of the event shall be recorded. The I&A subsystem may meet this requirement either through its own auditing mechanism or by providing an interface for passing the necessary data to another auditing mechanism.

Applicable Features

COMPSEC-II requires that users identify and authenticate themselves with a logon name and password before users are allowed access to the system upon which COMPSEC-II is installed.

COMPSEC-II assigns a unique user number to each user and associates this number in the audit log with all auditable actions taken by that user. COMPSEC-II does not provide for the audit logging of security relevant I&A events.

The authentication data is not sufficiently protected from unauthorized users. COMPSEC-II protects the authentication data through a DOS mechanism which hides the files, and fails to provide architectural protection from the subsystem.

Conclusion

COMPSEC-II fails to satisfy the D1 feature requirements for I&A.

Audit

Requirement

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identification and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, actions taken by computer operators and system administrators and/or system security officers, and other security relevant events. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity.

Interpretation

- D2:

The following subsections provide interpretations of the TCSEC requirements which shall be satisfied by auditing subsystems at AUD/D2.

2.4.3.1.1 Creation and management of audit trail

The auditing subsystem shall create and manage the audit trail of security-relevant events in the system. If the other portions of the system are unable to capture data about such events, the auditing subsystem shall contain the necessary interfaces into the system to perform this function. Alternatively, the auditing subsystem might simply accept and store data about events if the other portions of the system are capable of creating such data and passing them on.

2.4.3.1.2 Protection of audit data

It shall be demonstrated that the audit data is protected from unauthorized modification. This protection will be provided either by the subsystem itself or by its integration with the protected system.

2.4.3.1.3 Access control to audit

The audit mechanism, auditing parameters, and the audit data storage media shall be protected to ensure access is allowed only to authorized individuals. Individuals who are authorized to access the audit data shall be able to gain access only through the auditing subsystem.

2.4.3.1.4 Specific types of events

Data about all security relevant events must be recorded. The other portion of the system shall be able to pass data concerning these events to the auditing subsystem, or the auditing subsystem shall have the necessary code integrated into the other portions of the system to pass the data to the collection point.

2.4.3.1.5 Specific information per event

All of the specific information enumerated in the TCSEC quote shall be captured for each recorded event. Of particular concern, is the recording of the user identity with each recorded event.

2.4.3.1.6 Ability to selectively audit individuals

The auditing subsystem shall have the ability to perform selection of audit data based on individual users.

Applicable Features

COMPSEC-II creates an audit trail for security-relevant actions that take place on the system at the DOS command level. (See page 15 for a list of auditable events.) Appropriate data about each event is recorded in the audit trail including the date and time of the event, the

type of event and the success or failure of the event. The audit record includes the name of the object when appropriate. Through the use of post-selection on the audit trail, the system operator is able to perform selection of audit data based on individual users.

COMPSEC-II was found to be deficient in the following areas:

- The audit data files are encrypted and hidden using the DOS *attribute* facility. This does not provide adequate protection from reading by unauthorized users, from deletion or from modification.
- Security relevant actions taken by the system operator are not fully audited, only the activation of utility programs is reported.

Conclusion

COMPSEC-II fails to satisfy the D2 feature requirements for Audit.

Assurances

System Architecture

Requirement

The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system.

Interpretation

- D1:

This requirement applies to all subsystems evaluated at all classes, regardless of the function(s) they perform. There are two specific elements of this requirement: Execution Domain Protection and Defined Subsets.

3.1.1.1 Execution Domain Protection

Protection of the subsystem's mechanism and data from external interference or tampering must be provided. The code and data of the subsystem may be protected through physical protection (e.g., by the subsystems dedicated hardware base) or by logical isolation (e.g., using the protected system's domain mechanism).

3.1.1.2 Defined Subsets

I&A subsystems, when used for the system's I&A, define the subset of subjects under the control of the system's TCB.

DAC subsystems may protect a subset of the total collection of objects on the protected system.

- D2:

In the TCSEC quote, "TCB" is interpreted to mean "subsystem".

This requirement applies to all subsystems at the D2 class or the D3 class. The following interpretations explain how this requirement applies to specific functions performed by subsystems.

- Interpretation for DAC Subsystems:

All named objects which are in the defined subset of protected objects shall be isolated such that the DAC subsystem mediates all access to those objects.

- Interpretation for Auditing Subsystems:

The system's architecture shall ensure that the auditing mechanism cannot be bypassed by any subjects accessing those objects under the system's control.

- Interpretation for Object Reuse Subsystems:

The notion of subsetting objects is not applicable to object reuse subsystems. Object reuse subsystems shall perform their function for all storage objects on the protected system that

are accessible to users.

- Interpretation for I&A Subsystems:

This requirement aplies to I&A subsystems. Authentication data shall be protected from unauthorized access. Access to the authentication data shall also be recorded in the audit trail.

Applicable Features

It would appear that COMPSEC-II meets the requirement for execution domain protection because the subsystem has a dedicated hardware base, the COMPSEC-II hardware card. Problems in system architecture arise because a PC based system running DOS is a single-state machine and commercially available software exists which provides direct controller access from any executable file. Therefore, all subsystem owned objects that are necessarily part of the subsystem are not protected by the subsystem architecture. For some of these objects (files), the system uses the DOS technique of hiding the file and encrypting the information on the file. Although DES encryption certainly adds assurance that these subsystem files are not easily readable from outside the subsystem, this is insufficient protection to meet the CSSI architecture requirement. The only architectural protection for these objects is the use of a DOS mechanism whereby files are hidden and are not reported as present through a typical DOS command (dir). However, hiding a file provides no architectural protection afforded by the subsystem. Furthermore, commercially available routines exist to extract information from the hard disk even though it is hidden. COMPSEC-II can not prevent tampering with these files and tampering would not be audited, therefore COMPSEC-II does not meet the requirement for execution domain protection.

DAC

Any user can access any file on the hard disk if that file has not been brought under the control of COMPSEC-II through the use of an editor by the administrator. If an uncontrolled user file is an executable which allows access to the hard disk controller, then access is afforded to subsystem named objects. The file on the hard disk may not easily be changed in such a way that the subsystem will mistakenly use alterred information, since these files are DES encrypted. However, these files can be accessed without DAC subsystem mediation, which precludes COMPSEC-II from meeting the architecture requirement for DAC.

Audit

COMPSEC-II fails the architecture requirement for Audit because audit data is not isolated from interference from outside the subsystem. This data is protected on the hard disk through DES encryption and the DOS feature of hiding files. This technique is insufficient protection since the subsystem can not isolate these objects from outside the subsystem.

Object Reuse

COMPSEC-II overwrites deleted files and when a user logs off or a new user logs on, a full reboot is performed which clears RAM, registers, and buffers. Object reuse protection is not provided for removable media. Therefore, access to floppy disk drives must be restricted to the system operator or a procedure must be enforced that requires that all floppy disks be degaussed or otherwise erased before they are issued to users.

Identification and Authentication

COMPSEC-II fails the architecture requirement for identification and authentication because the subsystem can not isolate authentication data from tampering and access to authentication data is not audited.

Conclusion

COMPSEC-II fails to satisfy the D1 requirement for System Architecture.

System Integrity

Requirement

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

Interpretation

In the TCSEC quote, "TCB" is interpreted to mean "subsystem".

- D1:

This requirements applies to all subsystems evaluated at any class, regardless of the functions they perform.

- D2:

There are no additional requirements for System Integrity at D2.

Applicable Features

COMPSEC-II is shipped with a reasonably complete test suite. Test procedures are described in a document titled, "ATP Checklist For Testing COMPSEC-II Products". Test procedures are organized by activity (e.g. initialization, disk drive testing, journal functionality testing). Individual test procedures which validate the operation of the hardware and firmware elements of the subsystem are listed:

- Firmware on the COMPSEC-II hardware card
- Memory on the COMPSEC-II hardware card is tested
- Screen addressability is tested
- Time-of-day clock is tested across reboots
- Floppy drive operation is tested
- Encryption and decryption is tested

A.C.S.I. Inc. provides comprehensive tests to verify the correct installation and operation of their add-on hardware and their software.

Conclusion

COMPSEC-II satisfies the D2 System Integrity requirement.

Security Testing

Requirement

The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the TCB. Testing shall also include a search for obvious flaws that would allow violation of resource isolation, or that would permit unauthorized access to the audit or authentication data.

Interpretation

- D1:

This requirement applies to all subsystems evaluated at any class, regardless of the function(s) they perform. In the TCSEC quote, "TCB" is interpreted to mean "subsystem".

The subsystem's Security Relevant Portion (SRP) shall be tested and found to work as claimed in the subsystem's documentation. The addition of a subsystem to a protected system shall not cause obvious flaws to the resulting system.

Test results shall show that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the subsystem's SRP.

- D2:

This requirement applies to the testing of the SRP of any subsystem evaluated at the D2 class or the D3 class.

Applicable Features

The evaluation team tested COMPSEC-II in two phases, the first focusing on functional testing and then a second phase of security testing. The functional testing phase concentrated on assuring the team that the product was installed properly and functioned consistently with the instructions provided. Functional testing involved testing of the system as it might be installed in the field using DOS and any application programs that are not specifically

forbidden by the instructions. All optional security features were turned on and several accounts were created for each member of the evaluation team. For the security testing phase, COMPSEC-II was installed to provide the maximum security available with the product. This phase focused on determining if there were any apparent ways to bypass or defeat the security mechanisms.

All tests were performed on an IBM-PC operating under DOS version 3.30. The IBM-PC was configured with two floppy disk drives and a 20MB hard drive.

Functional Testing

The system works as documented in the Operations Manual which is for the most part well organized. However, the terminology used throughout the documentation can be very misleading. (See page 40, Evaluator's Comments.)

Tests were conducted to ensure that no one can access the system without providing a valid user name and password. A user can not change the system date and time by using the DOS *date* and *time* commands. However, there was a bug in the clock that came with the system. While the clock was running, at the end of each month when the month changed, the year also changed where it was incremented by one. For example, the clock went from July 31, 1990 to August 1, 1991.

Tests of the audit mechanism included attempts to subvert or bypass the mechanism itself, attempts to corrupt the audit data, and an attempt to overflow the audit data storage area. The system denies a user access to the system when the allotted audit space becomes full. A review of the audit log showed that complete and correct data was written to the audit log for all events that were audited. However, information about security relevant actions taken by the system operator such as adding or deleting users, changing a user's access to a file, or changes made to the system clock are not included in the audit log.

Tests of the DAC mechanism showed that users cannot access files with DOS commands or from within high-level language executables when access has been denied through COMPSEC-II's DAC mechanism. Additionally, a user cannot use DOS commands to change access to a file where that access has been denied through COMPSEC-II's DAC mechanism.

Testing of the object reuse mechanism included deleting a file and then searching the disk to determine that the file had indeed been overwritten. Upon inspection of a recovered file, it appeared to be overwritten with random characters.

Security Testing

The second phase of testing, security testing, consisted of exercising the system and looking for obvious flaws that would bypass or defeat COMPSEC-II's protection mechanisms. Application programs, debuggers, utilities, and some locally written programs using DOS, BIOS, and absolute port addressing features were used for these tests.

Introducing such programs to a protected system may require a significant amount of work, depending on how well the system is managed, but once on the system, COMPSEC-II is not able to protect itself or system resources. (See page 40, Evaluator's Comments, for a description of the protection of resources on a single-state machine.)

The two audit logs; the file containing user numbers, logon names, and passwords; and the file that contains user access information all reside in the root directory. The DAC mechanism is not used to protect these files. The sole means of preventing a user from viewing, modifying or deleting these files is that these files are encrypted and hidden using the DOS attribute feature. Users cannot unhide these files or obtain any information about them through the use of this attribute feature.

The COMPSEC-II utilities are maintained in a directory that is by default protected using the COMPSEC-II DAC mechanism. Users cannot use any DOS commands to gain access to this directory and are thus prevented from viewing, executing, modifing, or deleting any files in this directory at the DOS or BIOS level.

Using absolute port addressing, a user is able to gain access to any file or memory location including the audit logs; the file which contains security switch settings; and the file which contains user number, logon name, and password information.

Conclusion

COMPSEC-II fails to satisfy the D1 Security Testing requirement.

Documentation

Security Features User's Guide

Requirement

A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, guidelines on their use, and how they interact with one another.

Interpretation

- D1:

All subsystems shall meet this requirement in that they shall describe the protection mechanisms provided by the subsystem.

- D2:

There are no additional requirements at the D2 Class.

Applicable Features

Once a user has logged on to the system, COMPSEC-II provides transparent security operation to the user. The introduction section of the Operations Manual gives an overall description of the protection mechanisms that COMPSEC-II offers. These protection mechanisms include the Logon, Password, Boot Control, Discretionary Access Control, and Encryption capabilities. Chapter 3 of the Operations Manual, "Configuration", describes the configuration switches that are available that the user may need to know about if the switches are turned on by the system operator such as Automatic Keyboard Time-out and Dual Key Logoff.

The Encryption feature is the only COMPSEC-II feature which the user can directly use if granted that privilege by the system operator. When the system operator is entering the user Logon information in the Logon Control Menu, there is an "encryption" prompt to which the System Operator must enter "yes" or "no" for each user. A "yes" will give that

user encryption privilege allowing that user to operate the Manual Encryption/Decryption and Message Authentication facilities. Using these facilities, this user can then encrypt files to which the user has access. Chapter 7 of the Operations Manual, "Crypto", instructs the user how to use the Manual Encryption Facilities.

Unless there is a special need to allow a user to encrypt files, the ability to encrypt files should be limited to system operator. Having the ability to encrypt files requires that the user have access to the COMPSEC-II directory, even though the user will only be allowed to use the Manual Encryption Facilities.

Even though COMPSEC-II is transparent to the user, there are a few system messages that the user should be familiar with. The COMPSEC-II User's Quick Reference section of Appendix G in the Operations Manual describes these messages.

Within the Operations Manual, COMPSEC-II documents the protection mechanisms provided and guidelines on their use. The user is given guidance on available features, instructions on how to login to the system and a description of the COMPSEC-II messages that the user may see.

Conclusion

COMPSEC-II satisfies the D2 Security Features User's Guide requirement.

Trusted Facility Manual

Requirement

A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility.

Interpretation

- D1:

This requirement applies to all subsystems in that the manual shall present cautions about functions and privileges provided by the subsystem. Further, this manual shall present specific and precise direction for effectively integrating the subsystem into the overall system.

- D2:

This requirement applies directly to all auditing subsystems and to other subsystems that maintain their own audit data concerning events that happen under their control. For subsystems that create audit data and pass it to an external auditing collection and maintenance facility, the audit record structure shall be documented; however, the procedures for examination and maintenance of audit files may be left to the external auditing facility.

Applicable Features

The Operations Manual is addressed to the system operator presenting cautions when running a secure facility. The manual states instructions for installation and configuration of COMPSEC-II on the system. It presents the COMPSEC-II features and guides the system operator through the use of each feature. Chapter 6 of the Operations Manual, "Journal", is adequate in describing the procedures for analysis of the audit files and providing a description of the audit file structure. The Operations Manual is adequate in its instruction to the system operator in configuring the identification and authentication and audit features for secure operation. Object reuse is enforced only if the system operator enables the System Reboot switch. The COMPSEC-II Operations Manual is clear in stating that if the System Reboot switch is disabled object reuse is not enforced, however, it should also state that the system operator must enable the System Reboot switch to meet the object reuse D2 security requirements.

One of the D2 DAC requirements is to provide the capability to restrict DAC to the granularity of a single user. COMPSEC-II enforces DAC by groups, not by users. However, if the system operator is told that in the assignment of groups, a group may contain only one user, then COMPSEC-II would meet the D2 DAC granularity requirement. (See page 19 for a description of single-user access granularity.)

The Operations Manual describes options that are available to the system operator in initializing COMPSEC-II. The Operations Manual instructs the system operator to select Boot Protection to specify the drive that the system will always use for booting. By selecting drive C, users are prevented from using a DOS bootable diskette on a floppy drive to boot the system and thereby bypass the COMPSEC-II protection mechanisms. The Operations Manual then instructs the System Operator to select "Set" to drive C, which will provide no access to drive C if the COMPSEC-II board is removed. The only way to retrieve the system is by the system operator logging on and providing the SYS.ID. The Operations Manual describes the SYS.ID as an option, a way of customizing an individual computer. However, in actuality, during installation of COMPSEC-II the SYS.ID is required. The Operations Manual should be corrected to reflect the actual system.

In initializing COMPSEC-II, the Operations Manual is adequate in instructing the system operator on which options to choose, as stated above. However, the Operations Manual is not as instructive in informing the system operator how to set the switches. It does inform the system operator what each switch does, however, it does not tell the system operator the exact switch settings to operate securely at D2. How some switches are set is truly at the discretion of the system operator, because they do not affect security, however others must be set a certain way.

System reboot must be enabled to meet the object reuse security requirements. The Low Level Access protection must be set to "Direct Disk Access Blocked" to enforce the Identification and Authentication requirements. This will prevent direct access to the disk, bypassing DOS and COMPSEC-II. Automatic Group 9 Logon must be disabled because I&A and individual accountability is not enforced on the users that automatically log on with group 9 access rights.

The Trusted Facility Manual is addressed to the system operator and presents cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event is given in the Trusted Facility Manual. However, the Trusted Facility Manual is not adequate in presenting specific and precise direction in setting the COMPSEC-II switches to effectively integrate the subsystem into the overall system and meet the D2 security requirements.

Conclusion

COMPSEC-II fails to satisfy the D1 Trusted Facility Manual requirement.

Test Documentation

Requirement

The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and results of the security mechanisms' functional testing.

Interpretation

- D1:

The document shall explain the exact configuration used for security testing. All mechanisms supplying the required supporting functions shall be identified. All interfaces between the subsystem being tested, the protected system, and other subsystems shall be described.

- D2:

There are no additional requirements at the D2 class.

Applicable Features

The COMPSEC-II test documentation consists of procedures and test results of installation, utility operation, and security mechanisms. However, the test documentation is not sufficient in identifying all interfaces between the subsystem being tested, the protected system, and perhaps other subsystems. The test documentation lacks system integrity tests. There are no tests to validate the correct operation of all hardware and firmware elements of the system regardless of whether they reside within the subsystem, the protected system, or other interfacing subsystems.

Conclusion

COMPSEC-II fails to satisfy the D1 Test Documentation requirement.

Design Documentation

Requirement

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.

Interpretation

- D1:

This requirement applies directly to all subsystems. Specifically, the design document shall state what types of threats the subsystem is designed to protect against (e.g., casual browsing, determined attacks, accidents). This documentation shall show how the protection philosophy is translated into the subsystem's SRP. Design documentation shall also specify how the subsystem is to interact with the protected system and other subsystems to provide a complete computer security system. If the SRP is modularized, the interfaces between these modules shall be described.

- D2:

There are no additional requirements for Design Documentation at the D2 class.

Applicable Features

The Operations Manual includes a description of COMPSEC-II's philosophy of protection and how this philosophy is translated into COMPSEC-II. However, there is no design documentation that describes the interfaces between the COMPSEC-II modules and between COMPSEC-II and the protected system.

Conclusions

COMPSEC-II fails to satisfy the D1 Design Documentation requirement.

Rating Assignment

This section describes the composite rating and how it is determined. A composite rating is assigned to each evaluated feature and is based on the individual ratings assigned in Chapter 3. The individual ratings are the rating for each feature and ratings for the assurance and documentation supporting that feature. The chart below shows a 'Y' for each assurance or documentation requirement that is sufficient to support the rating of each feature. An 'N' indicates that the assurance or documentation requirement is not sufficient. For features

that have a rating of 'D', the assurances and documentation requirements are irrelevant, and are marked 'N/A'. Using the ratings attained in Section 3, the composite ratings for each of COMPSEC-II's features are derived as shown in the following table.

Evaluated Features	Feature Rating	Assurance			Documentation				Support Function	Composite Rating
		Arch.	Integrity	Testing	SFUG	TFM	Test	Design		
I&A	D	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Audit [1] DAC [2]	D
Audit	D	N/A	N/A	N/A	N/A	N/A	N/A	N/A	I&A [3] DAC [2]	D
DAC	D2	N	Y	N	Y	N	N	N	I&A [3]	D
OR	D2	N	Y	N	Y	N	N	N	I&A [4]	D

The CSSI requires that subsystems have *supporting functions* because some features rely on one another (e.g. an auditing subsystem needs user identities from the I&A subsystem). The CSSI permits a subsystem to accomplish this by alternative methods:

- the supporting function is provided by another feature of the subsystem
- the supporting function is provided within the feature even though it may duplicate an aspect of another feature
- the supporting function is provided through an interface to other products

If the supporting function is integrated within the product, it must be at the same level as that of the feature to obtain the composite rating.

[1] Audit logging of security relevant I&A events is required at D2.

[2] Audit and I&A data are protected through DAC.

[3] The DAC and Audit mechanisms get user IDs from the I&A mechanism.

[4] The OR mechanism gets user IDs from the I&A mechanism.

Evaluator's Comments

This section allows the evaluators to comment on features or problems that the TCSEC and CSSI do not specifically address. This provides a "hands on" perspective which a user of a system may find useful or needs to administer or use the system.

COMPSEC-II appears to be a reasonably sound attempt to provide security controls on an IBM PC compatible system running DOS. Unfortunately, this single-state machine does not provide inherent separation between user processes and the portions of the operating system which must be trusted for security features to be non-bypassable. This problem, along with the commercial availability of software designed to debug system problems on these systems, creates a system with no assurance that security features have not been bypassed. Security products on these types of systems, like COMPSEC-II, unfortunately create a false sense of security because they are carefully implemented and do provide security features in demand. It is this inherent system flaw that caused most of the mechanism failures of COMPSEC-II during this evaluation.

Evaluated Hardware Components

This appendix lists the A.C.S.I. Inc. marketing identification numbers for all hardware covered by this evaluation. This list is equivalent to the set of hardware officially supported by the evaluation. The primary requirement for hardware is that the hardware function properly.

To operate in correspondence with the DAC, object reuse, I&A, and audit ratings, the security subsystem must contain the hardware components listed in this section.

The protected systems covered by this evaluation include IBM-PC, XT, AT, and 100% compatible machines running DOS versions 2.0 through 3.3. The system that was used during this evaluation was an IBM-PC with a 20 MB hard disk and two DS/DD floppy disk drives.

The COMPSEC-II hardware card is marked with the product name and company name as well as a copyright notice dated 1986, 1987, 1988. The hardware card has a 3V lithium battery, a bank of four dip switches, and 14 integrated circuits installed and labeled as follows:

U1 DALLAS DS1210 8916C1

U2 KM6264AL-10 813 KOREA

U3 CD74HCT163E RCA H 619

U4 +B8824 MM58167AN

U5 CD74HCT374E RCA H 724

U6 KM6264AL-10 813 KOREA

U7 US74HCT02 4384

U8 WDC'85 WD20C03-PH 10-10 8848 0023678465

U9 CD74HCT245E RCA H 701

U10 LATTICE GAL16V8-15LPS 881309

U11 CD74HCT245E RCA H 701

U12 CD74HCT10E RCA H 724

U13 LATTICE GAL16V8-15LPS 881309

U14 CD74HCT245E RCA H 701

The version number, B3.1, was not noted on the hardware card.

Evaluated Software Components

This section lists the programs that make up COMPSEC-II's software. COMPSEC-II is designed to run under DOS versions 2.0 through 3.3.

Version B3.1 of the COMPSEC-II software was evaluated. The software was delivered on one 5-1/4" floppy diskette. The software consisted of the files listed below. [1]

Filename	Date
ACD.SYS	03-25-90
ACD.EXE	03-25-90
CHECKCRC.EXE	12-14-88
CHMOD.EXE	02-16-87
COMPSEC.EXE	04-10-90
COMPSEC.ROM	03-25-90
CRCS.DIR	03-16-90
CRYPT.EXE	03-25-90
FREEZE.EXE	03-25-90
INSTALLH.EXE	03-25-90
LOGOFF.EXE	03-25-90
MAKECRC.EXE	12-14-88

[1]Note: Dates are listed with each filename because A.C.S.I. Inc. did not change version numbers when they updated the COMPSEC-II utilities.

Acronyms

ADP	Automatic Data Processing
BIOS	Basic Input-Output System
CSSI	Computer Security Subsystem Interpretation
CPU	Central Processing Unit
DAC	Discretionary Access Control
DES	Data Encryption Standard
DoD	Department of Defense
DOS	Disk Operating System
EPL	Evaluated Products List
I&A	Identification and Authentication
MS-DOS	MicroSoft Disk Operating System
NCSC	National Computer Security Center
OR	Object Reuse
PC	Personal Computer
RAM	Random Access Memory
ROM	Read Only Memory
SRP	Security Relevant Portion
TCB	Trusted Computing Base
TCSEC	Trusted Computer Security Evaluation Criteria
TFM	Trusted Facility Manual

* U.S. Government Printing Office : 1991 - 617-699/41071

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT UNLIMITED DISTRIBUTION
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) CSC-EPL--SUM-91/004	5. MONITORING ORGANIZATION REPORT NUMBER(S) S236,004
6a. NAME OF PERFORMING ORGANIZATION National Computer Security Center 6b. OFFICE SYMBOL (If applicable) C71	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State and ZIP Code) 9800 Savage Road Ft. George G. Meade, MD 20755-6000	7b. ADDRESS (City, State and ZIP Code)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State and ZIP Code)	10. SOURCE OF FUNDING NOS. PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT NO.
11. TITLE (Include Security Classification) Final Evaluation Report ACSI COMPSEC-II	
12. PERSONAL AUTHOR(S) Barbara A. Maguschak, Cynthia Reese, Robert L. Williamson	
13a. TYPE OF REPORT Final 13b. TIME COVERED FROM _____ TO___	14. DATE OF REPORT (Yr, Mo., Day) 91,06,10 15 PAGE COUNT 44
16 SUPPLEMENTARY NOTATION	

17. COSATI CODES		
FIELD	GROUP	SUB. GR.

18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
NCSC, I&A, DAC, AUD, CSSI, OR, American Computer Security Industries, Inc., COMPSEC-II USA American Version, release B3.1

19. ABSTRACT (Continue on reverse side if necessary and identify by block number)
The National Computer Security Center (NCSC) examined the security protection mechanisms provided by American Computer Security Industries, Incorporated's COMPSEC-II USA American Version, release B3.1. COMPSEC-II is a subsystem, not a complete trusted computer system. Therefore, it was evaluated against the *Computer Security Subsystem Interpretation* (CSSI). Specifically, the applicable requirements for this evaluation included Identification & Authentication (I&A), Discretionary Access Control (DAC), audit, and object reuse. The evaluation team determined that the highest class at which COMPSEC-II satisfies the I&I, DAC, audit and object reuse requirements of the CSSI is class D. This report documents the findings of the evaluation.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED	
22a. NAME OF RESPONSIBLE INDIVIDUAL PATRICIA L. MORENO	22b TELEPHONE NUMBER (Include Area Code) (301)859-4458	8b OFFICE SYMBOL C71

DD FORM 1473, 83 APR EDITION OF 1 JAN 73 IS OBSOLETE.

☆ U.S. Government Printing Office : 1991 - 617-699/41071